



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/720,353

12/21/2000

Michael Nolte

6400-11WOUS

1134

7590

07/24/2006

McCormick Paulding & Huber
City Place II
185 Asylum Street
Hartford, CT 06103-4102

EXAMINER

POLTORAK, PIOTR

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 07/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/720,353

Applicant(s)

NOLTE, MICHAEL

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 May 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The Amendment, and remarks therein, received on 5/02/06 have been entered and carefully considered. Additionally the acknowledgment is made of the receipt of the certified copy of the German application.
2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

Applicant's arguments have been carefully

3. As per claim 11 applicant argues disagrees with the examiner's statement that a control center and a sender are both within a transmitter.

Although the examiner disagrees with provided arguments the examiner agrees that the newly introduced amendment "wherein the control center, the receiver, and the sender are individual and separate one from the other" overcomes the art of record.

4. As per claim 8 applicant argues that Horstmann does not "cure the deficiencies" of Hoffmann and that Horstmann is "merely seen to disclose a mechanism for use in electronic software distribution that provides purchase documentation and allows for re-download and re-licensing of software".

The examiner carefully considered applicant's argument but respectfully disagrees with applicant's position. As pointed out in the previous Office Action Horstmann contains the list of already used numbers and rejects already used numbers. The feature of keeping track of used numbers (whether tickets or sequence numbers) prevent replay attacks and thus introducing Horstmann's list into Hoffman's invention

would have been obvious to one of ordinary skill in the art at the time of applicant's invention.

5. As per claim 14 applicant argues that Hoffman '012 discloses "a unique hardware identification code and sequence number which increases by one for each transmission rather than disclosing the sequence number being comprised of one of decreasing numbers, numbers with a step interval greater than unity and numbers representing data and time".

The examiner carefully considered applicant's argument but respectfully disagrees with applicant's position. As discussed in the previous Office Action Hoffman '012 discloses changing numbers in sequence for each transmission and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the sequence number being comprised of one of decreasing numbers, numbers with a step interval greater than unity and numbers representing data and time, the time including a number of seconds from an appointed start time given the benefit of keeping track of the transactions.

6. As per claims 10 and 15 applicant contests the Official Notice but does not provides any concrete arguments to the contrary.
7. As per applicant arguments and amendments the 35 USC § 112 first and second paragraph rejection have been withdrawn.

However, as per claim 11 the examiner pointed out that it was not clear whether there was a problem with the written description, or understanding of the specification and claim language. Specifically, the examiner underlined the fact that

the claim language suggested some inconsistency in light of prior art, well known computing knowledge and understanding of the specification.

Claim 11 recites creation of a signature that is verified against a calculated signature.

The signature is created using a key and a sequence number.

The signature key is equivalent to a check key that is derived in a similar fashion to a signature key (using a main key and a sequence number).

However, the calculated signature (that is used to verify the signature) is derived using only the check key without use of the sequence number.

The claim language (or rather the lack of) is consistent with the specification that also does not provide teaching of using the sequence number and the check key for calculated signature creation.

8. Since, applicant clarified that the claim language was correct and the process of creating signature differs from the process of verification the signature, where the process of signature creation includes additional variable (a sequence number) that is not present in signature verification (the sequence number is only present in creating the check key but not in creating the calculated signature) the 35 USC § 112 second paragraph rejection is withdrawn. However, the clarification of the matter that contradicts the examiner's interpretation of the claim language introduces a new 35 USC § 112 first paragraph rejection and subsequently applicant should explain how two essentially identical entities (the signature and corresponding the calculated signature) can be verified since creation of one entity (the signature)

involves an additional variable (a sequence number) not present in creation of the other entity (the calculated signature).

9. Note that the examiner recognizes that a sequence number is used in signature as well as the calculated key creation. However, this particular detail was omitted in the paragraph above in effort to better present the science problem identified by the examiner.

10. Claims 2-17 have been examined.

Claim Rejections - 35 USC § 112

11. Claim 2-8 and 11-17 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement and the written description requirement.

The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

As per claim 11 it is not clear how two essentially equivalent signature are created with use of non equivalent variables. In particular, it is not clear how the signature created with a signing key and sequence number can be verified with a calculated signature that is derived using just a check key and no sequence number.

Claim 9 contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. "The inputs of the signature checker are further connected to an output of a second one-

Art Unit: 2134

time encrypter for providing a check key” being part of a control center critical or essential to the practice of the invention, but not included in the claim(s) is not enabled by the disclosure. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976). Specifically, the one-time encrypter is part of a control center (clearly shown in claim 9 lines 3-4 and suggested in lines 13-15) and the signature checker is part of a receiver (clearly shown in claim 9 lines 6-7).

Claims 2-8, 10 and 12-17 are rejected by virtue of their dependence.

Clarification is required.

12. Claims 2-9 and 12-17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.

13. The amended claim language of claim 9 is not understood and as a result the metes and bounds of the claim is uncertain. Claim 9 previously recited: “the inputs of the signature checker are further connected to an output of a second one-time encrypter for providing a check key”. The language as cited was consistent with the prior art and suggested that there are two one-time encrypters first in the control center and the second in the receiver. The signature checker in the receiver would use the key derived from the second one-time encrypter to check signature. However, the newly introduced amendment: “the inputs of the signature checker are further connected to an output of the one-time encrypter for providing a check key” is not clear especially

in light of another new introduced amendment that underlines that the control center and the receiver are individual and separate one from the other.

Specifically, it is not clear whether the claim language: "the inputs of the signature checker are further connected to an output of the one-time encrypter for providing a check key, whose inputs are connected to the second memory of the receiver for the secret main key and to a means for determining a sequence number for the received data message block ..." suggests that the input of the signature checker that is stored in the receiver is connected to an input of the one time encrypter that is stored in the control center, or whether the "whose inputs" is directed to the check key.

14. Applicant states that the control center, the receiver, and the sender are individual and separate one from the other. However, the claim language "the signature checker are further connected to an output of the one-time encrypter" that the claim suggest that the signature checker (that is part of the receiver) is an extension of the one-time encrypter (that is part of the control center) rather than that the output of the one-time encrypter is an input of the signature checker.

15. Claims 2-8 and 12-17 are rejected by virtue of their dependence.

Clarification is required.

16. If applicant were to amend claim 9, applicant is encouraged to simplify the claim language. The current claim structure is difficult to follow and to clearly identify how presented elements are "interconnected". See for example the following: "The

inputs of the signature checker are further connected to an output of the one-time encrypter for providing a check key, whose inputs are connected to the second memory of the receiver for the secret main key and to a means for determining a sequence number for the received data message block, the check key and the determined sequence number being used to derive the check key that is used to form a calculated signature for comparison to the signature of the data message block".

Also, the examiner reminds applicant that terms such as "for" are intended use terms. A claim containing a "recitation with respect to the manner in which a claimed apparatus is intended to be employed does not differentiate the claimed apparatus from a prior art apparatus" if the prior art apparatus teaches all the structural limitations of the claim. *Ex parte Masham*, 2 USPQ2d 1647 (Bd. Pat. App. & Inter. 1987).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not


Art Unit: 2134


mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


7/17/06


JACQUES LOUIS JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100